# Une communication bayésienne et intelligente pour l'Internet des Objets

Cristanel Razafimandimby, Valeria Loscrì, Anna Maria Vegni, Alessandro Neri

# *Une communication bayésienne et intelligente pour l'Internet des Objets*

Cristanel Razafimandimby[1] † et Valeria Loscrí[1] et Anna Maria Vegni[2] et Alessandro Neri[2]

[1] *Inria Lille - Nord Europe, Lille, France*
[2] *Department of Engineering, Roma Tre University, COMLAB Telecommunication Laboratory, Rome, Italy*

L'Internet des Objets (IdO) a obtenu un grand succès dans divers domaines d'application. Toutefois, malgré ce succès, l'un des plus grands défis à relever est la grande quantité de données générées par les dispositifs de capteur. Cela peut affecter la consommation d'énergie et causer la congestion du réseau. Pour resoudre ce probleme, nous proposons dans cet article une Approche d'Inférence Bayésienne (AIB) permettant d'éviter la transmission des données fortement corrélées. AIB est basé sur une architecture hiérarchique composée de simple capteurs, de passerelles intelligentes et de centre de données. L'Algorithme Belief Propagation est utilisé pour reconstituer les données manquantes. La solution proposée est évalué sur la base des données recueillies sur des capteurs réels. Sur les divers scénarios étudiés, les résultats montrent que notre approche réduit considerablement le nombre de données transmises et la consommation d'énergie tout en maintenant une qualité d'information acceptable.

**Mots-clefs :** IoT, Belief Propagation, Markov Random Fields, Cloud, Smart Gateway

## 1 Introduction

Despite of the large success of IOT, one major challenge that should be addressed is the huge amount of data generated by the sensing devices. Storing this big data locally and even temporarily will not be possible any more. Therefore, harnessing cloud computing capacity is needed, but unfortunately this is not enough. However, it was observed that, with the increase of sensor density, data generated by IoT devices tend to be highly redundant. Thus, uploading raw data to the cloud can become extremely inefficient due to the waste of memory and network overloading.

To address this issue, either the IoT devices should avoid the generation of useless data or a gateway device should be able to stop uploading of redundant data from some devices, to reduce consumption of network and cloud resources.

From the above considerations, in this paper we present a Bayesian Inference Approach (BIA), which allows to remove a great amount of spatio-temporal correlation data in an IoT domain. BIA is based on Pearl's Belief Propagation (BP) algorithm which is an iterative technique mostly used for solving inference problems [YFW03]. A good correlation between data is important in such inference problems since it dictates the accuracy of data inference, and hence reduces the estimation error of the global information.

## 2 Network Model

As depicted in FIGURE 1, in this paper we propose a BP approach in a cloud-based architecture consisting of simple nodes, smart gateways and data centers. Each entity in our architecture plays a different role w.r.t the functionalities, the computational and communication capabilities. Our IoT network model may include multiple subnets associated with different applications. Each subnet is composed of IoT devices connected to each others for data sharing, and a smart gateway that relays the data flows to the cloud. The cloud in turn is responsible of inference, storage and all the cloud-based services.

†This work was partially supported by a grant from CPER Nord-Pas-de-Calais/FEDER Campus Intelligence Ambiante

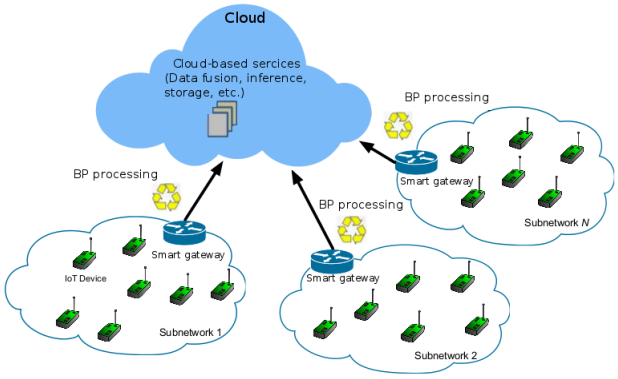


FIGURE 1: A cloud-based IoT network model.

In a given IoT application, the sensor nodes periodically collect environmental data, such as temperature, humidity and illumination, and forward them to the gateways using a multi-hop routing protocol. Then, the gateways collect the data and decide what has to be sent to the cloud. This decision depends on the fact whether the gateway knows or not the *a priori* probability of inference error of the used approach.

# 3 Bayesian Inference Approach

In this section, we describe our BIA technique which is based on Pearl's BP algorithm that will be described below.

**I) Model :** As a starting point before any inference procedure, the design of a graphical model should be provided. Graphical models are schematic representations of probability distributions. They consist of nodes connected by either directed or undirected edges. Each node represents a random variable, and the edges represent probabilistic relationships between variables. Models which are comprised of directed edges are known as *Bayesian networks*, whilst models that are composed of undirected edges are known as *Markov random fields* (MRF).

As in [VLNL16], we present an inference approach under the hypothesis of MRF, modeled by means of Factor Graphs. It follows that our goal is to estimate the state $X$ of the sensed environment starting from the sets of data collected by each sensor node. If $X$ is modeled as a MRF, by taking advantage of the Hammersley-Clifford Theorem, the joint probability distribution of $X$ with a set of cliques ‡ $C$ is given by $p_X(x) = \frac{1}{Z} exp\{-E(x)\}$, where $Z$ is the normalization factor, and $E(x) = \sum_{c \in C} \psi_c(x_c)$ is the energy function, $\psi_c$ is the potential associated with clique $c \in C$, and $x_c$ is the set of nodes belonging to the clique indexed by $c$.

**II) Belief Propagation :** Once the model has been defined, queries can be performed on the model to find the marginal probability distribution for one node or a set of nodes in the network graph. We use BP algorithm for this purpose and also for the computation cost reason. BP is a well known algorithm for performing inference on graphical models [YFW03]. In general, we assume that some observations are made and some other data about the underlying environment will be inferred. The choice of data to infer is based on the strong correlation between data.

Given the $i$-th device, let us denote with $\varepsilon_i$ the observation of the phenomenon we intend to share (e.g. temperature) and with $x_i$ the random variable associated to the phenomenon we want to infer, (e.g. humidity).

If we associate each IoT device of our subnet with a random variable $X_i$, which represents the local information (such as temperature and humidity), the joint probability can be written as :

$$P_X(x) = \prod_i \psi_i(x_i) \quad \prod_{i,j \in E} \psi_{ij}(x_i, x_j), \tag{1}$$

‡. Clique is defined as a fully connected subset of nodes in the graph.

where $\psi_i(x_i)$ is the evidence function, $E$ is the set of edges encoding the statistical dependencies between two nodes $i$ and $j$, and $\psi_{ij}()$ represents the potential function. Note that the graphical model parameters (i.e. $\psi_i$ and $\psi_{ij}$) can be estimated from the observed data by using a learning algorithm like in [Gha02].

We recall that $p(x_i)$ represents the marginal distribution of $i$-th node, and the BP allows the computation of $p(x_i)$ at each node $i$ by means of a message passing algorithm. The message from node $i$ to $j$ related to the local information $x_i$ is defined as :

$$m_{ji}(x_i) \propto \int \psi_{ji}(x_j, x_i)\psi_j(x_j) \prod_{u \in \Gamma(j), u \neq i} m_{uj}(x_j)dx_j, \tag{2}$$

where $\Gamma(j)$ denotes the neighbors of node $j$ and the incoming messages from previous iteration are represented by $m_{uj}$.

Eq. (2) will be performed between all nodes in the model until the convergence will be reached. Thus, the prediction *i.e.*, the belief at each $i$-th node, is computed through all the incoming messages from the neighboring nodes and the local belief, *i.e.* :

$$\hat{x_i} = belief(x_i) = k\psi_i(x_i) \prod_{u \in \Gamma(i)} m_{ui}(x_i) \tag{3}$$

where $k$ is a normalization constant.

It is worth to mentioning that the BP is able to compute the exact marginalization in the case of tree-structured graphical models.

# 4 Evaluation & discussion of the results

## 4.1 Experimental Setup

In this section we provide the experimental results of our approach. Real data collected from 54 sensors deployed in the Intel Berkeley Research lab have been used [PBT]. These sensors collect temperature, humidity, light and voltage of node battery readings, as well as the network connectivity information which makes possible to reconstruct the network topology. Each data collection has been performed every 30 seconds. The original data consists of 38 days of readings. However, we will focus only on the first three hours of readings in this work. After computing the Pearson correlation among data subset, we noticed that there is a good correlation between temperature and humidity data. Hence, we can easily infer the humidity data from temperature data and vice versa. In this paper, we decided to infer humidity from temperature. The temperature is in degrees Celsius, whilst the humidity is a value ranging from 0-100%.

We assess our approach w.r.t. (*i*) the number of transmitted data, (*ii*) the energy consumption (EC), (*iii*) the average value of the distortion level, and (*iv*) the average value of the estimation error (ER).

The distortion level allows us to determine the difference between the real and the estimated value. The distortion level can be expressed using the Mean Squared Error (MSE) metric.

All of our assessments are based on three different scenarios. In scenario $s1$, the gateway sends to the cloud all the temperature and humidity data it receives. This means that the cloud does not perform any inference. In the second scenario $s2$, the gateway sends only the temperature data to the cloud, and the cloud in turn infers the corresponding humidity data by using the BP algorithm. Finally, in the scenario $s3$, we consider that the gateways are "smart" devices, meaning that before sending their data to the cloud, they first compute the probability $p(e|T,h)$ of making an inference error $e$ on the cloud given the temperature $T$, and the humidity $h$. If there is a strong chance that the error magnitude exceeds a predefined threshold (0.5 in our case), the gateway send both humidity and temperature data to the cloud, else the gateway send only the temperature data, and the humidity value will be inferred in the cloud using the BP algorithm. The computation of $p(e|T,h)$ is done by means of the BP algorithm also. It should be noted that this computation requires the knowledge of the a priori probability of inference error, *i.e.*, $p(e)$.

As you may have noticed, with the proposed scenarios above, removing the redundancy data at the gateway has no effect on the sensing nodes since they do not filter the data. However, it is interesting to study the possibility of doing the raw data filtering in the sensing nodes. By doing that, not only the large

| *Scenario* | *#Transmitted data* | *EC* (Wh) | *MSE* | *ER* |
|---|---|---|---|---|
| s1 | 20346 | 854.532 | - | - |
| s2 | 10173 | 427.266 | 0.04 | 0.26 |
| s3 | 12496 | 524.832 | 0.02 | 0.037 |

TABLE 1: Results obtained during the first three hours of readings.

computation and the single point of failure at the gateways will be avoided but also the energy consumption of sensing nodes will probably decreased. The energy costs reported in TABLE 1 is therefore the estimated energy costs assuming that data filtering will be done on the sensing nodes and the used model is exactly the same as on the gateways. In our energy consumption evaluations, we assume that the power consumption for sending each temperature and humidity value is 14 mW. This cost has been obtained on the Mica2Dot Berkeley mote as reported by [AFP+04].

### *4.2 Obtained results*

Our approach was implemented in C++, and the assessments were performed with respect to the ground truth. TABLE 1 illustrates the obtained results during the first three hours of readings. We can notice that our Bayesian inference approach drastically reduces the number of transmitted data and the energy consumption, while maintaining an acceptable level of prediction accuracy and information quality.

We can notice also that we decrease considerably the estimation error by using the scenario s3. Indeed, the gateways are smarter in this case. By computing the a posteriori probability of inference error, they will be able to estimate the right moment and the data type to send in the cloud. However, this increases the number of transmitted data, as compared to scenario s2. This is due to the fact that in s2 gateways send only the temperature data without worrying of the risk of inference error in the cloud.

## 5 Conclusions

In this paper, we have presented a inference-based approach that allows avoiding transmitting useless data in an heterogeneous IoT network. The strong correlation between data was taken into account for this study. Through extensive simulations and by using the real data collected from 54 sensors deployed in the Intel Berkeley Research lab, we have showed that our Bayesian inference approach reduces considerably the number of transmitted data and the energy consumption, while keeping an acceptable level of estimation error and information quality. We have also shown that the use of smart gateway decreases significantly the inference error. Note that even though we used a data source from WSN to validate our approach, it can be easily applied to different types of data sources provided by IoT devices. Future works will explore the possibility of doing the raw data filtering in the sensing nodes.

## Références

[AFP+04] Giuseppe Anastasi, Alessio Falchi, Andrea Passarella, Marco Conti, and Enrico Gregori. Performance measurements of motes sensor networks. In *Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 174–181. ACM, 2004.

[Gha02] Zoubin Ghahramani. Graphical models : parameter learning. *Handbook of brain theory and neural networks*, 2 :486–490, 2002.

[PBT] W. Hong S. Madden M. Paskin P. Bodik, C. Guestrin and R. Thibaux. Intel lab data. *http ://www.select.cs.cmu.edu/data/labapp3/index.html*. Accessed July 20, 2016.

[VLNL16] Anna Maria Vegni, Valeria Loscri, Alessandro Neri, and Marco Leo. A bayesian packet sharing approach for noisy iot scenarios. pages 305–308, 2016.

[YFW03] Jonathan S Yedidia, William T Freeman, and Yair Weiss. Understanding belief propagation and its generalizations. *Exploring artificial intelligence in the new millennium*, 8 :236–239, 2003.